BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

PCM ok

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G07F 19/00, G06F 17/60, G07F 7/10 — A2

(11) International Publication Number: **WO 98/05011**

(43) International Publication Date: 5 February 1998 (05.02.98)

(21) International Application Number: PCT/US97/13673

(22) International Filing Date: 31 July 1997 (31.07.97)

(30) Priority Data:
08/692,907 31 July 1996 (31.07.96) US

(71) Applicant *(for all designated States except US)*: VERIFONE, INC. [US/US]; Suite 400, Three Lagoon Drive, Redwood City, CA 94065 (US).

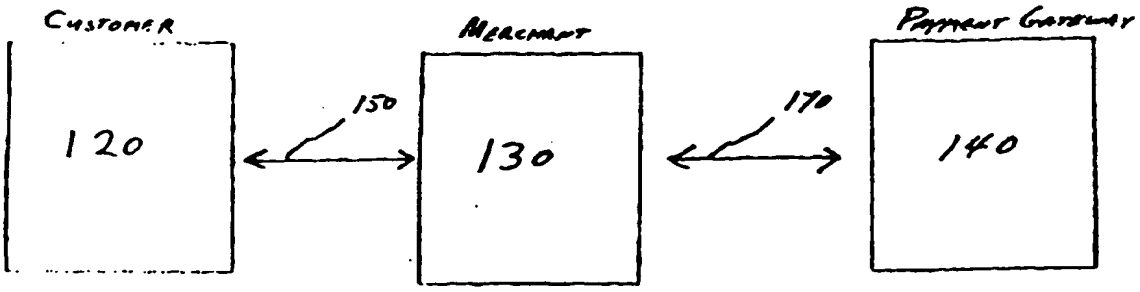
(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: ROWNEY, Kevin, T., B. [US/US]; 748 Duncan Street, San Francisco, CA 94131 (US).

(74) Agents: STEPHENS, L., Keith et al.; Warren, Perez & Stephens, Suite 710, 8411 Preston Road, Dallas, TX 75225 (US).

(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, HU, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, ARIPO patent (GH, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

Published
Without international search report and to be republished upon receipt of that report.

(54) Title: A SYSTEM, METHOD AND ARTICLE OF MANUFACTURE FOR SECURE, STORED VALUE TRANSACTIONS OVER AN OPEN COMMUNICATION NETWORK UTILIZING AN EXTENSIBLE, FLEXIBLE ARCHITECTURE



(57) Abstract

An architecture that provides a server that communicates bidirectionally with a gateway over a first communication link, over which service requests flow to the server for one or more merchants and/or consumers is disclosed. Service requests are associated with a particular merchant based on storefront visited by a consumer or credentials presented by a merchant. Service requests result in merchant specific transactions that are transmitted to the gateway for further processing on existing host applications. By presenting the appropriate credentials, the merchant could utilize any other computer attached to the Internet utilizing a SSL or SET protocol to query the vPOS system remotely and obtain capture information, payment administration information, inventory control information, audit information and process customer satisfaction information. Secure transmission of a value transfer protocol transaction is provided between a plurality of computer systems over a public communication system, such as the Internet. A connection is created between two computer systems using a public network, such as the Internet, to connect the computers. Then, digital certificates and a digital signature are exchanged to ensure that both parties are who they say they are. Finally, the two smart cards involved in a transaction are read by individual computers connected utilizing the network, and the value transfer protocol is executed over the secured network. The value transfer protocol facilitates the exchange of money between the two smart cards.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

A SYSTEM, METHOD AND ARTICLE OF MANUFACTURE FOR SECURE, STORED VALUE TRANSACTIONS OVER AN OPEN COMMUNICATION NETWORK UTILIZING AN EXTENSIBLE, FLEXIBLE ARCHITECTURE

Field Of The Invention

The present invention relates to the secure, electronic payment in exchange for goods and services purchased over a communication network, and more specifically, to a system, method and article of manufacture for securely transmitting value transfers from one smart card to another smart card over an open, communication network utilizing a flexible, extensible architecture.

The present invention relates to an electronic representation of a monetary system for implementing electronic money payments as an alternative medium of economic exchange to cash, checks, credit and debit cards, and electronic funds transfer. The Electronic-Monetary System is a hybrid of currency, check, card payment systems, and electronic funds transfer systems, possessing many of the benefits of these systems with few of their limitations. The system utilizes electronic representations of money which are designed to be universally accepted and exchanged as economic value by subscribers of the monetary system.

Today, approximately 350 billion coin and currency transactions occur between individuals and institutions every year. The extensive use of coin and currency transactions has limited the automation of individual transactions such as purchases, fares, and bank account deposits and withdrawals. Individual cash transactions are burdened by the need to have the correct amount of cash or providing change therefor. Furthermore, the handling and managing of paper cash and coins is inconvenient, costly and time consuming for both individuals and financial institutions.

Although checks may be written for any specific amount up to the amount available in the account, checks have very limited transferability and must be supplied from a physical inventory. Paper-based checking systems do not offer sufficient relief from the limitations of cash transactions, sharing many of the inconveniences of handling currency while adding the

inherent delays associated with processing checks. To this end, economic exchange has striven for greater convenience at a lower cost, while also seeking improved security.

Automation has achieved some of these qualities for large transactions through computerized electronic funds transfer ("EFT") systems. Electronic funds transfer is essentially a process of value exchange achieved through the banking system's centralized computer transactions. EFT services are a transfer of payments utilizing electronic "checks," which are used primarily by large commercial organizations.

The Clearing House (ACH) where a user can enter a pre-authorized code and download information with billing occurring later, and a Point Of Sale (POS) system where a transaction is processed by connecting with a central computer for authorization for the transaction granted or denied immediately are examples of EFT systems that are utilized by retail and commercial organizations. However, the payments made through these types of EFT systems are limited in that they cannot be performed without the banking system. Moreover, ACH transactions usually cannot be performed during off business hours.

Home Banking bill payment services are examples of an EFT system used by individuals to make payments from a home computer. Currently, home banking initiatives have found few customers. Of the banks that have offered services for payments, account transfers and information over the telephone lines using personal computers, less than one percent of the bank's customers are using the service. One reason that Home Banking has not been a successful product is because the customer cannot deposit and withdraw money as needed in this type of system.

Current EFT systems, credit cards, or debit cards, which are used in conjunction with an on-line system to transfer money between accounts, such as between the account of a merchant and that of a customer, cannot satisfy the need for an automated transaction system providing an ergonomic interface. Examples of EFT systems which provide non-ergonomic interfaces are disclosed in US Patents Numbers 5,476,259; 5,459,304; 5,452,352; 5,448,045; 5,478,993; 5,455,407; 5,453,601; 5,465,291; and 5,485,510.

To implement an automated, convenient transaction that can dispense some form of economic value, there has been a trend towards off-line payments. For example, numerous ideas have been proposed for some form of "electronic money" that can be used in cashless payment transactions as alternatives to the traditional currency and check types of payment systems. See U.S. Pat. No. 4,977,595, entitled "METHOD AND APPARATUS FOR IMPLEMENTING ELECTRONIC CASH," and U.S. Pat. No. 4,305,059, entitled "MODULAR FUNDS TRANSFER SYSTEM."

The more well known techniques include magnetic stripe cards purchased for a given amount and from which a prepaid value can be deducted for specific purposes. Upon exhaustion of the economic value, the cards are thrown away. Other examples include memory cards or so called smart cards which are capable of repetitively storing information representing value that is likewise deducted for specific purposes.

It is desirable for a computer operated under the control of a merchant to obtain information offered by a customer and transmitted by a computer operating under the control of the customer over a publicly accessible packet-switched network (e.g., the Internet) to the computer operating under the control of the merchant, without risking the exposure of the information to interception by third parties that have access to the network, and to assure that the information is from an authentic source. It is further desirable for the merchant to transmit information, including a subset of the information provided by the customer, over such a network to a payment gateway computer system that is designated, by a bank or other financial institution that has the responsibility of providing payment on behalf of the customer, to authorize a commercial transaction on behalf of such a financial institution, without the risk of exposing that information to interception by third parties. Such institutions include, for example, financial institutions offering credit or debit card services.

One such attempt to provide such a secure transmission channel is a secure payment technology such as Secure Electronic Transaction (hereinafter "SET"), jointly developed by the Visa and MasterCard card associations, and described in Visa and MasterCard's *Secure Electronic Transaction (SET) Specification*, February 23, 1996, hereby incorporated by reference. Other such secure payment technologies include Secure Transaction Technology ("STT"),

Secure Electronic Payments Protocol ("SEPP"), Internet Keyed Payments ("iKP"), Net Trust, and Cybercash Credit Payment Protocol. One of ordinary skill in the art readily comprehends that any of the secure payment technologies can be substituted for the SET protocol without undue experimentation. Such secure payment technologies require the customer to operate software that is compliant with the secure payment technology, interacting with third-party certification authorities, thereby allowing the customer to transmit encoded information to a merchant, some of which may be decoded by the merchant, and some which can be decoded only by a payment gateway specified by the customer.

Another such attempt to provide such a secure transmission channel is a general-purpose secure communication protocol such as Netscape, Inc.'s Secure Sockets Layer (hereinafter "SSL") , as described in Freier, Karlton & Kocher (hereinafter "Freier"), *The SSL Protocol Version 3.0*, March 1996, and hereby incorporated by reference. SSL provides a means for secure transmission between two computers. SSL has the advantage that it does not require special-purpose software to be installed on the customer's computer because it is already incorporated into widely available software that many people utilize as their standard Internet access medium, and does not require that the customer interact with any third-party certification authority. Instead, the support for SSL may be incorporated into software already in use by the customer, e.g., the Netscape Navigator World Wide Web browsing tool. However, although a computer on an SSL connection may initiate a second SSL connection to another computer, a drawback to the SSL approach is each SSL connection supports only a two-computer connection. Therefore, SSL does not provide a mechanism for transmitting encoded information to a merchant for retransmission to a payment gateway such that a subset of the information is readable to the payment gateway but not to the merchant. Although SSL allows for robustly secure two-party data transmission, it does not meet the ultimate need of the electronic commerce market for robustly secure three-party data transmission. Other examples of general-purpose secure communication protocols include Private Communications Technology ("PCT") from Microsoft, Inc., Secure Hyper-Text Transport Protocol ("SHTTP") from Terisa Systems, Shen, Kerberos, Photuris, Pretty Good Privacy ("PGP") which meets the IPSEC criteria. One of ordinary skill in the art readily comprehends that any of the general-purpose secure communication protocols can be substituted for the SSL transmission protocol without undue experimentation.

Banks desire an Internet payment solution that emulates existing Point of Sale (POS) applications that are currently installed on their host computers, and require minimal changes to their host systems. This is a critical requirement since any downtime for a banks host computer system represents an enormous expense. Currently, VeriFone supports over fourteen hundred different payment-related applications. The large number of applications is necessary to accommodate a wide variety of host message formats, diverse methods for communicating to a variety of hosts with different dial-up and direct-connect schemes, and different certification around the world. In addition, there are a wide variety of business processes that dictate how a Point of Sale (POS) terminal queries a user for data and subsequently displays the data. Also, various vertical market segments, such as hotels, car rental agencies, restaurants, retail sales, mail sales / telephone sales require interfaces for different types of data to be entered, and provide different discount rates to merchants for complying with various data types. Moreover, a plethora of report generation mechanisms and formats are utilized by merchants that banking organizations work with.

Banks are unwilling to converge on "standards" since convergence would facilitate switching from one acquiring bank to another by merchants. In general, banks desire to increase the cost that a merchant incurs in switching from one acquiring bank to another acquiring bank. This is accomplished by supplying a merchant with a terminal that only communicates utilizing the bank's proprietary protocol, and by providing other value-added services that a merchant may not be able to obtain at another bank.

Internet-based payment solutions require additional security measures that are not found in conventional POS terminals. This additional requirement is necessitated because Internet communication is done over publicly-accessible, unsecured communication line in stark contrast to the private, secure, dedicated phone or leased line service utilized between a traditional merchant and an acquiring bank. Thus, it is critical that any solution utilizing the Internet for a communication backbone, employ some form of cryptography.

As discussed above, the current state-of-the-art in Internet based payment processing is a protocol referred to as SET. Since the SET messages are uniform across all implementations,

banks cannot differentiate themselves in any reasonable way. Also, since SET is not a proper superset of all protocols utilized today, there are bank protocols which cannot be mapped or translated into SET because they require data elements for which SET has no placeholder. Further, SET only handles the message types directly related to authorizing and capturing credit card transactions and adjustments to these authorizations or captures. In a typical POS terminal in the physical world, these messages comprise almost the entire volume of the total number of messages between the merchant and the authorizing bank, but only half of the total number of different message types. These message types, which are used infrequently, but which are critical to the operation of the POS terminal must be supported for proper transaction processing.

Recently, the Internet was proposed as a communication medium connecting personal computers with specialized reader hardware for facilitating reading and writing to smart cards. However, the Internet is not a secure communication medium and value transfer was not secured. Thus, a solution was necessary to shore up the Internet with secure value transfer processing to facilitate smart card processing over the Internet. In addition, support was required to ensure that no third party could hijack a value transfer transaction. This would occur if someone diverted the transaction before it even started. In the prior art face-to-face solution, both parties can confirm the other party's identity. However, the Internet separates the parties with miles of wire.

SUMMARY OF THE INVENTION

According to a broad aspect of a preferred embodiment of the invention, secure transmission of a value transfer protocol transaction is provided between a plurality of computer systems over a public communication system, such as the Internet. A connection is created between two computer systems using a public network, such as the Internet, to connect the computers. Then, digital certificates and a digital signature are exchanged to ensure that both parties are who they say they are. Finally, the two smart cards involved in a transaction are read by individual computers connected utilizing the network, and the value transfer protocol is executed over the secured network. The value transfer protocol facilitates the exchange of money between the two smart cards.

DESCRIPTION OF THE DRAWINGS

The foregoing and other objects, aspects and advantages are better understood from the following detailed description of a preferred embodiment of the invention with reference to the drawings, in which:

Figure **1A** is a block diagram of a representative hardware environment in accordance with a preferred embodiment;

Figure **1B** depicts an overview in accordance with a preferred embodiment;

Figure **1C** is a block diagram of the system in accordance with a preferred embodiment;

Figure **2** depicts a more detailed view of a customer computer system in communication with merchant system under the Secure Sockets Layer protocol in accordance with a preferred embodiment;

Figure **3** depicts an overview of the method of securely supplying payment information to a payment gateway in order to obtain payment authorization in accordance with a preferred embodiment;

Figure **4** depicts the detailed steps of generating and transmitting a payment authorization request in accordance with a preferred embodiment;

Figures **5A** through **5F** depict views of the payment authorization request and its component parts in accordance with a preferred embodiment;

Figures **6A** and **6B** depict the detailed steps of processing a payment authorization request and generating and transmitting a payment authorization request response in accordance with a preferred embodiment;

Figures **7A** through **7J** depict views of the payment authorization response and its component parts in accordance with a preferred embodiment;

Figure **8** depicts the detailed steps of processing a payment authorization response in accordance with a preferred embodiment;

Figure **9** depicts an overview of the method of securely supplying payment capture information to a payment gateway in accordance with a preferred embodiment;

Figure **10** depicts the detailed steps of generating and transmitting a payment capture request in accordance with a preferred embodiment;

Figures **11A** through **11F** depict views of the payment capture request and its component parts in accordance with a preferred embodiment;

Figures **12A** and **12B** depict the detailed steps of processing a payment capture request and generating and transmitting a payment capture request response in accordance with a preferred embodiment;

Figures **13A** through **13F** depict views of the payment capture response and its component parts in accordance with a preferred embodiment;

Figure **14** depicts the detailed steps of processing a payment capture response in accordance with a preferred embodiment;

Figure **15A** & **15B** depicts transaction processing of merchant and consumer transactions in accordance with a preferred embodiment;

Figure **16** illustrates a transaction class hierarchy block diagram in accordance with a preferred embodiment;

Figure **17** shows a typical message flow between the merchant, vPOS terminal and the Gateway in accordance with a preferred embodiment;

Figures **18A-E** are block diagrams of the extended SET architecture in accordance with a preferred embodiment;

Figure **19** is a flowchart of vPOS merchant pay customization in accordance with a preferred embodiment;

Figures **20A-20H** are block diagrams and flowcharts setting forth the detailed logic of thread processing in accordance with a preferred embodiment;

Figure **21** is a detailed diagram of a multithreaded gateway engine in accordance with a preferred embodiment;

Figure **22** is a flow diagram in accordance with a preferred embodiment;

Figure **23** illustrates a Gateway's role in a network in accordance with a preferred embodiment;

Figure **24** is a block diagram of the Gateway in accordance with a preferred embodiment;

Figure **25** is a block diagram of the vPOS Terminal Architecture in accordance with a preferred embodiment;

Figure **26** is an architecture block diagram in accordance with a preferred embodiment;

Figure **27** is a block diagram of the payment manager architecture in accordance with a preferred embodiment;

Figure **28** is a Consumer Payment Message Sequence Diagram *in* accordance with a preferred embodiment of the invention;

Figure **29** is an illustration of a certificate issuance form in accordance with a preferred embodiment;

Figure **30** illustrates a certificate issuance response in accordance with a preferred embodiment;

Figure **31** illustrates a collection of payment instrument holders in accordance with a preferred embodiment;

Figure **32** illustrates the default payment instrument bitmap in accordance with a preferred embodiment;

Figure **33** illustrates a selected payment instrument with a fill in the blanks for the cardholder in accordance with a preferred embodiment;

Figure **34** illustrates a coffee purchase utilizing the newly defined VISA card in accordance with a preferred embodiment of the invention;

Figure **35** is a flowchart of conditional authorization of payment in accordance with a preferred embodiment;

Figures **36-48** are screen displays in accordance with a preferred embodiment;

Figure **49** shows how the vPOS authenticates an incoming response to a request in accordance with a preferred embodiment;

Figure **50** is a flowchart for the merchant interaction with the Test Gateway in accordance with a preferred embodiment;

Figures **51-61** are flowcharts depicting the detailed logic of the gateway in accordance with a preferred embodiment;

Figure **62** is the main administration display for the Gateway in accordance with a preferred embodiment;

Figure **63** is a configuration panel in accordance with a preferred embodiment.

Figure **64** is a host communication display for facilitating communication between the gateway and the acquirer payment host in accordance with a preferred embodiment;

Figure **65** is a Services display in accordance with a preferred embodiment;

Figure **66** is a graphical representation of the gateway transaction database in accordance with a preferred embodiment; and

Figure **67** illustrates a payment architecture in accordance with a preferred embodiment.

DETAILED DESCRIPTION

A preferred embodiment of a system in accordance with the present invention is preferably practiced in the context of a personal computer such as the IBM PS/2, Apple Macintosh computer or UNIX based workstation. A representative hardware environment is depicted in Figure **1A**, which illustrates a typical hardware configuration of a workstation in accordance with a preferred embodiment having a central processing unit **10**, such as a microprocessor, and a number of other units interconnected via a system bus **12**. The workstation shown in Figure **1A** includes a Random Access Memory (RAM) **14**, Read Only Memory (ROM) **16**, an I/O adapter **18** for connecting peripheral devices such as disk storage units **20** to the bus **12**, a user interface adapter **22** for connecting a keyboard **24**, a mouse **26**, a speaker **28**, a microphone **32**, and/or other user interface devices such as a touch screen (not shown) to the bus **12**, communication adapter **34** for connecting the workstation to a communication network (e.g., a data processing network) and a display adapter **36** for connecting the bus **12** to a display device **38**. The workstation typically has resident thereon an operating system such as the Microsoft Windows NT or Windows/95 Operating System (OS), the IBM OS/2 operating system, the MAC OS, or UNIX operating system. Those skilled in the art will appreciate that the present invention may also be implemented on platforms and operating systems other than those mentioned.

A preferred embodiment is written using JAVA, C, and the C++ language and utilizes object oriented programming methodology. Object oriented programming (OOP) has become increasingly used to develop complex applications. As OOP moves toward the mainstream of software design and development, various software solutions require adaptation to make use of the benefits of OOP. A need exists for these principles of OOP to be applied to a messaging interface of an electronic messaging system such that a set of OOP classes and objects for the messaging interface can be provided.

OOP is a process of developing computer software using objects, including the steps of analyzing the problem, designing the system, and constructing the program. An object is a software package that contains both data and a collection of related structures and procedures. Since it contains both data and a collection of structures and procedures, it can be visualized as a self-sufficient component that does not require other additional structures, procedures or data to perform its specific task. OOP, therefore, views a computer program as a collection of largely autonomous components, called objects, each of which is responsible for a specific task. This concept of packaging data, structures, and procedures together in one component or module is called encapsulation.

In general, OOP components are reusable software modules which present an interface that conforms to an object model and which are accessed at run-time through a component integration architecture. A component integration architecture is a set of architecture mechanisms which allow software modules in different process spaces to utilize each others capabilities or functions. This is generally done by assuming a common component object model on which to build the architecture.

It is worthwhile to differentiate between an object and a class of objects at this point. An object is a single instance of the class of objects, which is often just called a class. A class of objects can be viewed as a blueprint, from which many objects can be formed.

OOP allows the programmer to create an object that is a part of another object. For example, the object representing a piston engine is said to have a composition-relationship with the object representing a piston. In reality, a piston engine comprises a piston, valves and many

StreetAddress1=800 El Camino Real\n
StreetAddress2=Suite 400\n
City=Menlo Park\n
StateProvince=CA\n
Country=USA\n
PostOfficeBox=\n
ZipPostalCode=94025\n
\n

An empty line indicates the end of *AVSData*.
The detailed information that is available for the Address Verification Service depends on the Payment Window that captures the data from the consumer.

AVS Data (LEGACY-only)
For "LEGACY" version "1.0" only the *ZipPostalCode* name value pair is required. The Gateway will only use the first 5 characters of this value.

Transaction Replay Attacks

The processing of Internet-based payment transactions is a coordinated interaction between the Internet Transaction Gateway and the vPOS servers that is based on the following principles. A vPOS terminal, as the initiator of the payment transaction, is responsible for the round-trip logical closure of the transaction. vPOS will retry a transaction that has been initiated with the Gateway but where the response for the request was never received from the Gateway. A vPOS terminal selects -- out of a pre-assigned range -- a ***Terminal-Id*** that is to be used by the Gateway in a request to the host processor. This data element must be transported from the vPOS to the Gateway along with the payment-related information. The ***Terminal-Ids*** must be unique among the concurrent vPOS instances on a vPOS server system. However, the ***Terminal-Ids*** have no history. For example, a subsequent Force Post transaction need not use the same ***Terminal-Id*** as the original Authorization transaction. The vPOS will be responsible for making sure that only one request is outstanding for the same ***<Merchant-id, Terminal-id>*** data elements from a vPOS server system. The Gateway does not know that a response

was successfully received by vPOS. This means that the vPOS must be responsible for initiating any retry attempts. The Gateway never initiates a retry attempt with the host processor without an explicit retry request from vPOS. The Gateway when asked to retry a request with the host, performs a relational database look-up and delivers a response that has already been received from the host processor but was previously missed by vPOS. This behavior of the Gateway is also known as the "transaction response cache." The Gateway will need to know that a vPOS request is a retry of something already sent. The prior request may or may not have been received. A solution for determining the difference between a retry attempt and a new request was described earlier in this document. vPOS must understand the "canonical" error codes that it will receive via the Gateway and be able to initiate the proper recovery action and/or generate the appropriate user-interface dialog.

Certificate Processing

Merchants require a mechanism for verifying legitimate cardholders is of valid, branded bankcard account numbers. A preferred embodiment utilizes technology to link a cardholder to a specific bankcard account number and reduce the incidence of fraud and thereby the overall cost of payment processing. Processing includes a mechanism that allows cardholder confirmation that a merchant has a relationship with a financial institution allowing it to accept bankcard payments. Cardholders must also be provided with a way to identify merchants they can securely conduct electronic commerce. Merchant authentication is ensured by the use of digital signatures and merchant certificates.

In a preferred embodiment, a holder of a payment instrument (cardholder) surfs the web (Internet) for required items. This is typically accomplished by using a browser to view on-line catalog information on the merchant's World Wide Web page. However, order numbers can be selected from paper catalogs or a CD-ROM and entered manually into the system. This method allows a cardholder to select the items to be purchased either automatically or manually. Then, the cardholder is presented with an order form containing the list of items, their prices, and totals. The totals could include shipping, handling and taxes for example. The order form is delivered electronically from the merchant's server or created on the cardholder's computer by electronic shopping software. An alternative embodiment supports a negotiation for goods by presenting frequent shopper identification and information about a competitor's prices.

Once the price of goods sold and the means of payment has been selected, the merchant submits a completed order and the means for payment. The order and payment instructions are digitally signed by cardholders who possess certificates. The merchant then requests payment authorization from the cardholder's financial institution. Then, the merchant sends confirmation of the order, and eventually ships the goods or performs the requested services from the order. The merchant also requests payment from the cardholder's financial institution.

Figure **1C** is a block diagram of a payment processing system in accordance with a preferred embodiment. The Certificate Issuance at the Bank Web Site **162** resides at the bank web site **182**. It is utilized for issuing SET complaint / X.500 certificates to consumers. The implementation of this system may vary from one bank to another. However, the system gathers consumer's personal information, and after processing the information, the system issues a certificate along with a payment instrument to the consumer.

The Single Account Wallet **160** at the bank web site **182** represents the MIME message that is created by the Certificate Issuance system. This MIME message contains a VeriFone wallet. The VeriFone wallet contains a single payment instrument and the certificate associated with it. For security reasons, the private key is not included in the wallet. The has to specify a private key before using the instrument for payment. When the consumer is issued the certificate, this MIME message is sent to the browser. The browser launches the Certificate Installation application **174, 144** which is defined as a helper application in the browser. The Certificate Installation application **174, 144** reads the MIME message and install the wallet into the wallet database **158**.

Various helper applications **198, 172, 174, 176** are provided to make the consumer's shopping experience easy and efficient including the following helper applications. The Paywindow helper application **188** is utilized by the consumer to authorize the payment to the merchant, to administer their wallets, to review their previously completed payment transactions and to perform housekeeping activities on the wallets. This application is defined as a 'helper'

application on the consumer's desktop. The browser launches this application when the merchant system sends a MIME message requesting payment.

The PayWindow Setup Helper application **172** is used by the consumer to install helper applications and other modules from the web site onto the consumer desktop. When a consumer attempts to install an application for a first time, the consumer does not have a helper application on the desktop. Thus, the first time installation of an application requires a consumer to perform two steps. First the user must download the system package to their desktop and then the user must run setup to decompress and install the system. Thereafter, whenever the consumer gets a new release of system software, the browser launches this helper application which in turn installs the appropriate other system modules.

The Certificate Installation Helper Application **174** is utilized to install a wallet that is issued by a bank. When the bank's certificate issuance web system sends the MIME message containing the VeriFone wallet, the browser launches this application. This application queries a consumer to determine if the payment instrument contained in the wallet is to be copied to an existing wallet or to be kept in the new wallet. This application then installs the payment instrument and the certificate into the wallet database **158**.

The Certificate Issuance CGI scripts **162** and the Single Account Wallet **160** at the Bank Web Site **182** is processed as described in the native system. The Certificate Installation Applet of the Bank Web Site **182** is utilized by the Certificate Issuance CGI scripts **162** system to deliver a consumer's certificate to the consumer's desktop.

Figure **26** is an architecture block diagram in accordance with a preferred embodiment of the subject invention. Processing commences at function block **2600** where the Graphical User Interface (GUI) part of the application is initialized. The GUI application **2600** provides the consumer with support for ordering and making payments during the shopping process. There are also GUI components provided for wallet creation; importing, certificate and payment method creation and maintenance; and for transaction register review and reporting. The screen designs, and their associated logic, for the helper applications and applets are individually discussed in detail below.

The Certificate Manager **2604** manages the automatic downloading of a consumer's certificate from a bank, validation of a consumer's and a merchant's certificates and automatic requisition of certificate renewal.

The Payment Manager **2606** coordinates and completes the payment request that is received from the merchant system. The payment request is received via a MIME message in the native code implementation or via an applet in the Java implementation. The payment request received contains the final GSO, Ship-To name, merchant certificate, merchant URL, coupons and the payment amount. The manager **2606** then communicates with the payment related GUI component to interact with the consumer to authorize and complete the payment transaction. The manager is also responsible for determining the payment protocol based on the consumer's payment instrument and the merchant's preferred payment protocol.

The manager **2606** includes a well defined Application Programming Interface (API) which enables OEMs to interface with the payment manager **2606** to make payments to specific HTTP sites. The detailed logic associated with the payment manager **2606** is presented in Figure **27**.

The payment manager **2606** enforces standard operations in the payment process. For example the receipt and the transaction record can automatically be transferred to the Wallet file once the payment is completed. The payment manager architecture in accordance with a preferred embodiment is presented in Figure **27**. A user interfaces with the payment manager **2730** via a user interface **2700** that responds to and sends a variety of transactions **2710**, **2708**, **2706**, **2704** and **2702**. The transactions include obtaining the next record, payment record, receipt, acceptance of the payment instrument and GSO components. In turn, the payment manager **2730** sends transactions **2714** and receipts **2720** to the wallet manager **2722** and receives payment instruments, certificates and private keys from the wallet manager **2722**.

The payment manager **2730** also sends and receives transactions to the protocol manager **2770** including a merchant's payment message **2760**, a consumer certificate and PK handle **2750**, a merchant URL **2742**, a payment **2740**, a signed receipt **2734** and a GSO, Selected

Payment Protocol and Selected Payment Instrument **2732**. The payment manager **2730** also accepts input from the payment applet or MIME message from the merchant as shown at function block **2780**. One aspect of the payment processing is a Consumer Payments Class Library (CPCL) **2770** which encapsulates the payment protocols into a single API. By encapsulating the payment protocols, applications are insulated from protocol variations. A SET Protocol provides an implementation of the client-side component of the Secure Electronic Transaction (SET) Protocol. A complete implementation of the client-side component of the CyberCash micro-payment protocol is also provided.

The Wallet Manager **2722** provides a standard interface to the wallet. It defines the wallet database structures and the payment instrument data structures, controls the access to the wallet and provides concurrency checking if more than one application attempts to open the same wallet. The interface to the wallet manager **2722** is published to allow OEMs to interface with the wallet manager and access the wallet database.

The wallet manager consists of the following sub-components:

Wallet Access. This component provides an interface to read and write wallet information.

Transaction Manager. This component provides an interface to read and write transaction corresponding to a wallet into the wallet database.

Payment Instrument Manager. This component manager provides a common interface to the specific payment instrument access components.

Credit Card Access, Debit Card Access, Check Access. These components deal with a specific payment instrument.

A Data Manager provides storage and retrieval of generic data items and database records. It is assumed that data fields, index fields or entire data records can be marked as encrypted and the encryption process is largely automated. The data manager has no specific knowledge of database records appropriate to different payment methods. This layer is separated out so as to reduce changes required when new payment methods are introduced. However RSA key pairs and certificates might be considered as "simple" data types. This component also provides an abstraction which supports wallet files on computer disk or contained in smart cards.

The Open Data Base Connectivity (ODBC)/Java Data Base Connectivity (JDBC) component provides Data Base Connectivity where formal database components are required. An embodiment of the Smart Card Wallet allows wallet data to be stored and/or secured by a cryptographic token.

A preferred embodiment includes a single file or directory of files comprising a "wallet" which contains personal information and information about multiple payment methods with the preferred implementation. These payment methods (Visa cards, debit cards, smart cards, micro-payments etc.) also contain information such as account numbers, certificates, key pairs, expiration dates etc. The wallet is envisaged to also contain all the receipts and transaction records pertaining to every payment made using the wallet. A Cryptographic API component provides a standard interface for RSA and related cryptographic software or hardware. This support includes encryption, signature, and key generation. Choice of key exchange algorithm, symmetric encryption algorithm, and signature algorithm should all be configurable. A base class stipulates generic behavior, derived classes handle various semantic options (e.g. software based cryptography versus hardware based cryptography.)

The Cryptographic Software portion provides RSA and DES support. This may be provided utilizing the SUN, RSA or Microsoft system components depending on the implementation selected for a particular customer. Cryptographic Hardware creates a lower level API which can underpin the Cryptography API and be utilized to replace Cryptography Software with an off the shelf cryptography engine. The message sequence charts describe the flow of messages/data between the consumer, the browser and/or the various major components of the Semeru system. The major components of the system are the Merchant system which includes the vPOS, the PayWindow, and the Payment Gateway. The merchant system allows a consumer to shop, accept the payment transactions sent by the PayWindow application, and send payment transactions to the acquiring bank. The Consumer Payments Class Library (CPCL) module is a layer within the application which sends the payment transactions, securely, from the consumer to the merchant.

Figure **28** is a Consumer Payment Message Sequence Diagram in accordance with a preferred embodiment of the invention. The diagram presents the flow of messages between the

consumer, the browser, the merchant system, the PayWindow application, and CPCL. This message flow describes the payment process from the time an order is completed and the consumer elects to pay, to the time the payment is approved and the receipt is returned to the consumer. The difference between the Native implementation and Java implementation of the PayWindow application is in the delivery of the order information to the PayWindow. Once the order information is received by the PayWindow, the flow of messages/data is the same for both implementations. In the case of the Native implementation, the order information is delivered via a MIME message. This MIME message is sent to the PayWindow by the browser via a document file. In the Java implementation, the order information is delivered to the PayWindow by an applet. The merchant system sends an applet with the order information to the browser which in turn delivers the order to the PayWindow. Once the order is received, the PayWindow interacts with the consumer and the Protocol modules for the completion of the payment process.

Enters Order and Clicks Calculate Order **2820**

This message represent the consumer order entry and the clicking of the 'Calculate Order' button. The consumer's shopping experience is all condensed into this one message flow for the purpose of highlighting the payment process. The actual implementation of the shopping process varies, however, the purpose does not, which is the creation of the order.

Order **2830**

This message represents the order information which is sent by the browser to the merchant via an HTML form.

Payment Applet with GSO, PPPs, AIs, merchant certificate and URL **2840**

On receipt of the order, the merchant system calculates the payment amount. This message represents the HTML page which is sent by the merchant system detailing the payment amount along with the Java payment applet which contains the GSO, PPPs, AIs, merchant certificate and URL.

Run Payment Applet **2845**

The Java enabled browser runs the Payment applet. The applet displays a button called "Pay" for the consumer to click. This is embedded in the HTML page delivered by the merchant.

Clicks Pay **2850**

This message represents the clicking of the Pay button on the browser by the consumer after confirming the payment amount.

GSO, PPPs, AIs, merchant certificate and URL **2860**

This message represents the GSO, PPPs, AIs, merchant certificate and the merchant URL carried by the Java applet. The Java applet now delivers these to the PayWindow application.

Merchant certificate **2862**

This message represents the merchant's certificate which is sent to the CPCL module for checking the validity of the merchant.

Merchant's validity **2864**

The CPCL modules examines the merchant's certificate and send this message to the PayWindow indicating whether or not the merchant is a valid merchant.

Wallet, Payment Instruments **2866**

This message represents the wallets and payment instruments that is displayed to the consumer. Not all payment instruments from a wallet is shown to the consumer. Only the ones accepted by the merchant is shown.

Payment Instrument **2868**

This message represents the payment instrument selected by the consumer. This message is created in the current design when the user double clicks on the payment image in the "Select Payment Method" Window.

GSO **2870**

This indicates that the GSO is displayed to the consumer in the "Make Payment Authorization" screen.

Authorization of Payment **2872**

This message represents the authorization of the payment by the consumer. The consumer authorizes the payment by clicking the 'Accept' button on the "Payment Authorization" screen.

Decide Payment Protocol **2874**

Once the consumer authorizes the payment, the payment protocol is decided by PayWindow based on the merchant's Payment Protocol Preferences and the consumer selected payment instrument.

Payment Authorization **2875**

These messages represent the merchant's URL, the GSO, payment protocol (PP) to use, account number, certificate and the private key handle (PK) associated with the payment instrument which is sent to the protocol module.

GSO with Payment Authorization **2876**

This message represents the payment instructions which is sent by the protocol module to the Merchant system. The GSO, PI, consumer certificate and PK is packaged based on the payment protocol.

Signed Receipt **2878**

This message represents the digitally signed transaction receipt received by the protocol module from the merchant.

Save Receipt with hash value **2880**

The digitally signed transaction receipt is saved by the PayWindow for future reference.

Payment Successful **2882**

This indicates that the transaction receipt and the 'payment successful' have been displayed to the consumer.

Certificate Processing

A payment instrument must be certified by a "certificate issuing authority" before it can be used on a computer network. In the case of credit card payments, the issuer may be one of the

card issuing banks, but it might also be a merchant (eg SEARS), a transaction aquiring bank or an association such as VISA or Mastercard.

Payment instrument information is stored in the consumer's wallet. The certificate which authorizes the payment instrument will be stored along with that data in a secured database. The process of acquiring a certificate is described below. A certificate can be delivered to a consumer in a preconfigured wallet. The consumer receives a wallet which contains the certificate together with the necessary details associated with a payment instrument including a payment instrument bitmap which is authorized by a certificate issuing authority or the agencies represented by the issuing authority.

Obtaining a certificate

A consumer will deliver or cause to be delivered information to a certificate issuing authority. Figure **29** is an illustration of a certificate issuance form in accordance with a preferred embodiment. A user may fill out the form on-line, on paper and mail it in, or get his bank or credit card company to deliver it. The consumer delivered data will usually contain a public key belonging to a security key pair generated by consumer software. This information will normally be mailed to the consumer's address and actuated by a telephone call from the consumer. The certificate authority takes this information and uses it to validate that he is indeed entitled to use the payment method. This processing normally takes a few days to accomplish. Information will normally be exchanged with the organization issuing the payment method in the physical space if there is one, and with credit agencies. The certificate information is loaded into the consumer's software to enable payment processing to proceed online.

In some cases the consumer will be able to select details about a payment instument holder (wallet) he desires to own. This may be the icon representing a holder, the access password or other information. After creating the certificate, the issuing authority can use information received in the certificate application to create a custom payment instrument holder ready to use. This payment instrument holder will contain the following information. Payment instrument information including card number **2900** and expiration date **2902**. Personal

information including name **2904**, address **2906**, social security number **2908** and date of birth **2910**.

The associated certificate (eg X509 standard), an associated public key or in some cases public/private key pair (eg RSA), and an approved bitmap representing the payment instrument are provided to the requesting consumer. Figure **30** illustrates a certificate issuance response in accordance with a preferred embodiment. An approved bitmap for a VISA card is shown at **3000**. Also a default payment holder **3010** and a default payment holder name are provided with the certificate issuance. After the consumer aquires the payment instrument holder **3010**, the payment instrument holder is immediately visible to him in his collection of payment instrument holders. Figure **31** illustrates a collection of payment instrument holders in accordance with a preferred embodiment. The predefined payment instrument holder **3100** is the same JOHN's WALLET that was predefined based on defaults by the certificate issuance form. Figure **32** illustrates the default payment instrument bitmap **3200** associated with the predefined payment instrument holder **3210** resulting from the consumer filling in and obtaining approval for a VISA card.

Figure **33** illustrates a selected payment instrument with a fill in the blanks for the cardholder in accordance with a preferred embodiment. Next time the payment instrument holder is opened in a payment context the certificate issuing authorty's approved instrument bitmap can be used to select the payment instrument and utilize it to make purchases. Figure **34** illustrates a coffee purchase utilizing the newly defined VISA card in accordance with a preferred embodiment of the invention.

Figure **35** is a flowchart of conditional authorization of payment in accordance with a preferred embodiment. Processing commences at **3500** where the program initializes the connection betweeen the cardholder and the merchant for the purposes of shopping. After the cardholder completes shopping, a new SSL connection is established which provides authenticating information to the merchant. At this point the merchant is able to execute payment functionality (based on SSL or SET) conditionally, based upon the quality and character of the digital signature and the certificate used to validate said signature. Then, at function block **3510**, the cardholder selects the payment instrument for the particular transaction. Payment instruments could

include VISA, MASTERCARD, AMERICAN EXPRESS, CHECK, SMARTCARD or DEBIT CARDS. The payment method is then submitted to the merchant at function block **3520**. The merchant then initializes the SET connection to the acquiring bank at function block **3530** if the connection is not already established. Then, at function block **3540**, the certificate is submitted to the merchant from the acquiring bank. The certificate includes a public key portion and a private key used as an irrebutable digital signature to authenticate the parties to the transaction. The certificate also includes information on the level of credit risk which allows a merchant to conditionally decide on the authorization or rejection of credit under a particular payment instrument based on their risk level and the merchant's personal comfort level with the ability of the cardholder to pay. This processing has not previously been possible because the information returned from the authorizing bank did not include a level of credit risk a cardholder posed, it only contained credit rejected or approved.

A detailed description of the gateway internals is presented below in accordance with a preferred embodiment.

Gw_ClearSetRequestHandler

Figure **51** depicts a flow diagram for the GatewayClearSetRequestHandler routine. Execution begins in Step **5105**. In Step **5110** an SET analysis routine is called to analyze the SET request, as will be more fully disclosed below. Step **5110** sets a status flag indicating the next stage to be performed by the Gateway. In Step **5120** the Gateway checks to see whether the status is set to indicate that a response should be provided to the user. If so, execution proceeds to Step 5190, which ends the request handling routine and returns control to a calling routine, which then provides a response to the user. Otherwise execution proceeds to Step **5130**. In Step **5130**, the Gateway checks to see if the status is set to indicate that forward translation is required. Forward translation is necessary to translate an outgoing message into a format that can be understood by the host computer. If forward translation is indicated, execution proceeds to Step **5135**. In Step **5135**, the outgoing message is forwarded translated, as more fully disclosed below with respect to Figure **53**. If no forward translation is indicated, for example, if an already-translated transaction is being retried, execution proceeds to Step **5140**. In Step **5140**, the Gateway checks to see if the next step is communication to the host. If so, the Gateway proceeds to Step **5145**, and initiates host communication as will be more fully discussed below with respect to Figure **54**. If not, execution proceeds to Step

5150. In Step **5150**, the Gateway checks to see whether reverse translation is indicated. Reverse translation translates a response from a host into a format useable by the calling routine. If reverse translation is indicated, execution proceeds to Step **5155**, and the reverse translation is performed, as will be more fully discussed below with respect to Figure 55. In any case, after either forward translation in Step **5135**, host communication in Step **5145**, or reverse translation in Step **5155**, control returns to Step **5120** for further processing. As will be more fully disclosed below, the forward translation, host communication, and reverse translation routines manipulate status indicators to prevent the occurrence of an infinite loop.

The Gw_ClearSetRequestHandler routine as depicted in Fig. **51** may be implemented using the following C++ code:

```
int Gw_ClearSetRequestHandler(CPCLRequest*pRequest)

{
    gwAction            action;
    char                fatalError;

    CPCLCCRequest       *pVehicle = (CPCLCCRequest *) pRequest;
    CGW_Engine          *setTrans = (CGW_Engine *) pVehicle-
>GetContext();

    action = setTrans->AnalyzeSetRequest(pVehicle,&fatalError);

    while ( (action!=GW_PROCEED_TO_RESPOND)&& (!fatalError) ) {
        switch (action) {
         case GW_PROCEED_TO_FWD_XLAT:
            action = setTrans->TranslateForward(pVehicle);
            break;

         case GW_PROCEED_WITH_HOST_COMMS:
            action = setTrans->DoHostCommunication(pVehicle);
```

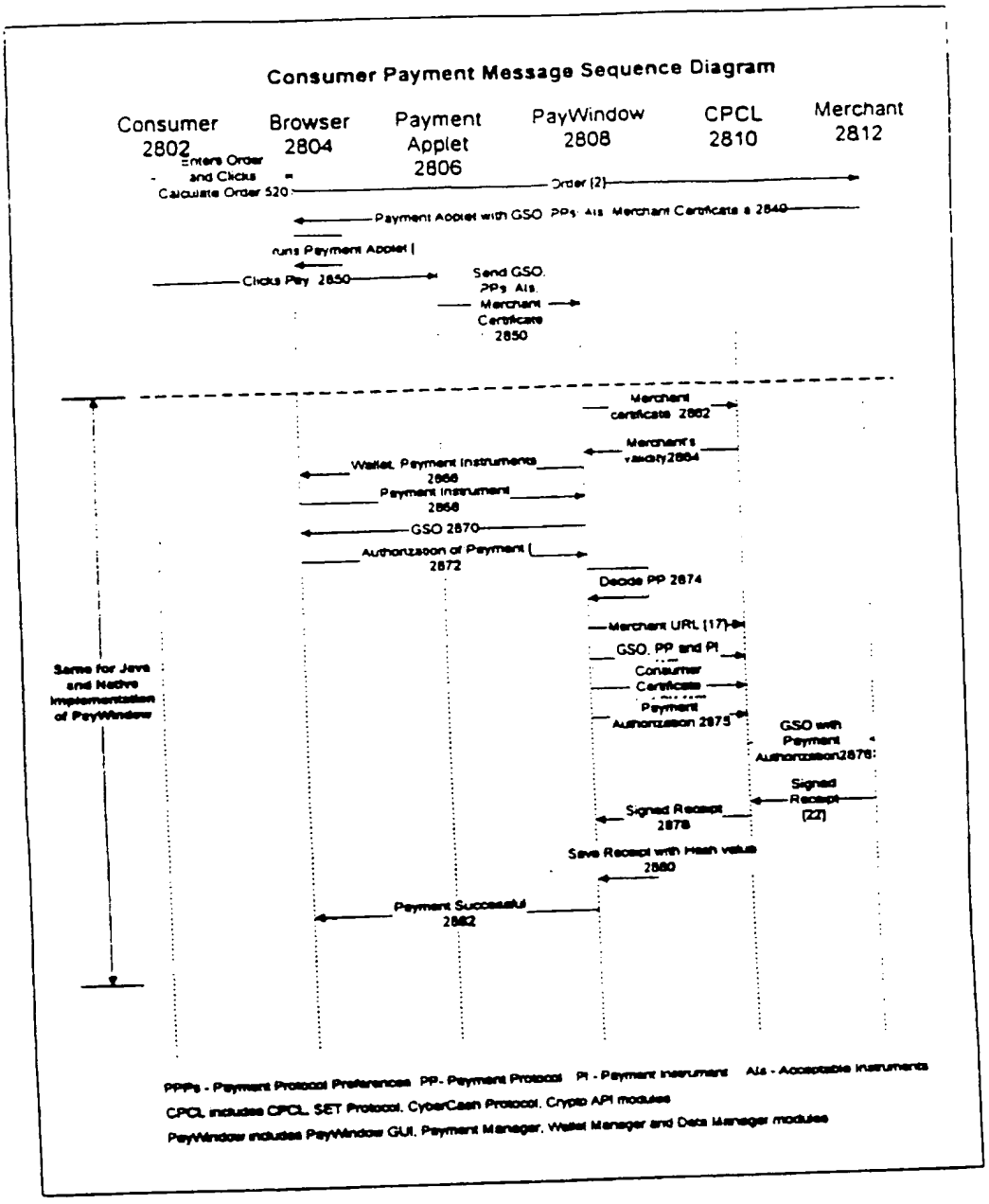

Consumer Payment Message Sequence Diagram
Consumer 2802
Browser 2804
Payment Applet 2806
PayWindow 2808
CPCL 2810
Merchant 2812
Enters Order and Clicks Calculate Order 520
Order (2)
Payment Applet with GSO PPs AIs Merchant Certificate s 2849
runs Payment Applet (
Clicks Pay 2850
Send GSO, PPs AIs, Merchant Certificate 2850
Merchant certificate 2862
Merchant's validity2864
Wallet, Payment Instruments 2866
Payment Instrument 2868
GSO 2870
Authorization of Payment (2872
Decide PP 2874
Merchant URL (17)
GSO, PP and PI
Consumer Certificate
Payment Authorization 2875
GSO with Payment Authorization2876
Signed Receipt (22)
Signed Receipt 2878
Save Receipt with Hash value 2880
Payment Successful 2882
Same for Java and Native Implementation of PayWindow
PPPs - Payment Protocol Preferences PP- Payment Protocol PI - Payment Instrument AIs - Accessible Instruments
CPCL includes CPCL, SET Protocol, CyberCash Protocol, Crypto API modules
PayWindow includes PayWindow GUI, Payment Manager, Wallet Manager and Data Manager modules

FIGURE 28